PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-276406
(43)Date of publication of application : 06.10.2000

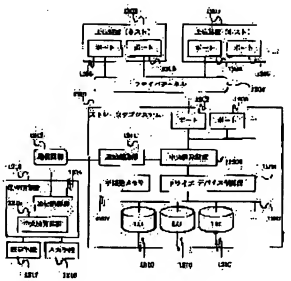
(51)Int.Cl. G06F 12/14
G06F 3/06

(21)Application number : 11-085393
(22)Date of filing : 29.03.1999

(71)Applicant : HITACHI LTD
(72)Inventor : OGASAWARA YUTAKA
OKAMI YOSHINORI

(54) FIBER CHANNEL CONNECTION STRAGE SUBSYSTEM AND ITS ACCESS MEMORY

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent illegal access by selectively limiting access from a host device to a storage area in a storage subsystem.
SOLUTION: The storage subsystem 1201 is connected to the host device 1203 by a port 1202 which has multiple fiber channel interfaces. The storage subsystem 1201 has a communication control part 1211 and sends and receives information to and from a communication control part 1214 of a device 1213 for maintenance through a communication line 1212 to maintain the storage subsystem 1201 and also set whether or not the host device 1203 is allowed to gain access by relating N-Port-Name and a specific storage area of LU 1210 with each other. Through the setting, access from the host device 1203 to the specific storage area in the storage subsystem 1201 is selectively limited. Consequently, illegal access can be prevented.



LEGAL STATUS

[Date of request for examination]	13.05.2002
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3744248
[Date of registration]	02.12.2005
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－276406
（Ｐ2000－276406Ａ）
(43)公開日　平成12年10月６日(2000.10.6)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｇ０６Ｆ　12/14	３２０	Ｃ０６Ｆ　12/14	３２０Ａ	５Ｂ０１７
3/06	３０１	3/06	３０１Ａ	５Ｂ０６５

審査請求　未請求　請求項の数５　ＯＬ　（全 14 頁）

(21)出願番号　特願平11－85393

(22)出願日　平成11年３月29日(1999.3.29)

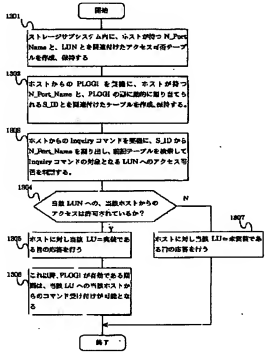
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　小笠原　裕
神奈川県小田原市国府津2880番地　株式会社日立製作所ストレージシステム事業部内
(72)発明者　岡見　吉規
神奈川県小田原市国府津2880番地　株式会社日立製作所ストレージシステム事業部内
(74)代理人　100068504
弁理士　小川　勝男

Ｆターム(参考)　５Ｂ０１７ ＡＡ０１ ＢＡ０１ ＢＢ０３ ＢＢ０６ ＣＡ０９
ＣＡ１６
５Ｂ０６５ ＣＡ０１ ＣＣ０１ ＰＡ０２ ＰＡ０４ ＰＡ１３

(54)【発明の名称】　ファイバチャネル接続ストレージサブシステム及びそのアクセス方法

(57)【要約】
【課題】ホストからストレージサブシステム内の記憶領域(LU)へのアクセスを選択的に制限することにより、不正アクセスを防止する。またこの際、アクセスの可否を判定する際生じるオーバヘッドが最小限となる方法を提供し、かつ判定の条件を標準ファイバチャネルプロトコルの範囲のみで行える方法を提供する。
【解決手段】ホストのN_Port_Name或いはNode_Nameとストレージサブシステム内のLUを関連付けるアクセス可否テーブル(1301)と、ホストがログインする際に割り当てるS_IDとLUとを関連付ける関連テーブル(1302)とを作成・保持し、ホストからのInquiry要求のS_IDと前記両テーブルとを用いてLUへのアクセス可否を判断し(1303)、ホストへ通知する(1304)。

図 18



【特許請求の範囲】
【請求項１】情報を記憶するドライブデバイスと、このドライブデバイスに情報を書き込み或いはこのドライブデバイスからの情報の読み込みを制御するデバイスドライブ制御部と、上位装置からのコマンドを受信するファイバチャネルインタフェースを持つポートと、前記コマンドに基づき前記デバイスドライブ制御部を制御して処理を行う演算装置とを備えたストレージサブシステムにおいて、
前記上位装置或いは上位装置のポートを識別する識別手段と前記ドライブデバイス内の特定の記憶領域とを関連付け前記上位装置から前記記憶領域に対するアクセス可否を定義したアクセス可否テーブルを設定するアクセス可否テーブル設定手段と、このアクセス可否テーブルを保持する保持手段とを備え、
前記演算装置は、前記上位装置からストレージサブシステムへの通信要求を受け付けた際にこの通信要求内の前記識別手段とフレームを送信するポートを識別するアドレス識別子とを関連付けた関連テーブルを設定し、この関連テーブルとドライブデバイスの実装状態を問い合わせるコマンドの前記アドレス識別子とから前記識別手段を割り出し、この識別手段と前記アクセス可否テーブルとから上位装置のアクセス可否を判断するストレージサブシステム。
【請求項２】前記演算装置は上位装置のアクセスを否と判断した場合には記憶領域が実装されていないという情報を上位装置に送信する請求項１に記載のストレージサブシステム。
【請求項３】情報を記憶するドライブデバイスと、このドライブデバイスに情報を書き込み或いはこのドライブデバイスからの情報の読み込みを制御するデバイスドライブ制御部と、上位装置からのコマンドを受信するファイバチャネルインタフェースを持つポートと、前記コマンドに基づき前記デバイスドライブ制御部を制御して処理を行う演算装置とを備えたストレージサブシステムにおいて、
前記上位装置からストレージサブシステムへの通信要求を受け付けた際にこの通信要求内の前記識別手段とフレームを送信するポートを識別するアドレス識別子とを関連付けた関連テーブルを設定する関連テーブル設定手段と、この関連テーブル及び前記上位装置或いは前記上位装置のポートを識別する識別手段と前記ドライブデバイス内の特定の記憶領域とを関連付け前記上位装置から前記記憶領域に対するアクセス可否を定義したアクセス可否テーブルとを保持する保持手段と、ドライブデバイスの実装状態を問い合わせるコマンドの前記アドレス識別子と前記関連テーブルとから割り出した前記識別子と前記アクセス可否テーブルとから上位装置のアクセス可否を判断する判断手段とを備えたストレージサブシステム。
【請求項４】前記アクセス可否テーブルは前記ポート毎に作成する請求項１乃至３の何れか1項に記載のストレージサブシステム。
【請求項５】前記上位装置或いは上位装置のポートを識別する識別手段とドライブデバイス内の特定の記憶領域とを関連付けこの記憶領域に対する上位装置のアクセス可否テーブルを作成・保持し、
前記上位装置からストレージサブシステムへの通信要求を受け付けた際に前記識別手段とフレームを送信するポートを識別するアドレス識別子とを関連付けた関連テーブルを作成・保持し、
この関連テーブルを用いてドライブデバイスの実装状態を問い合わせるコマンドの前記アドレス識別子から前記識別手段を割り出し、
割り出した識別手段と前記アクセス可否テーブルとを比較して前記上位装置のアクセス可否を判断するストレージサブシステムのアクセス方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ANSI X3T11で標準化されたファイバチャネルプロトコルを、上位装置とのインタフェースとして持つストレージサブシステム（ディスクサブシステム）に係り、複数の上位装置からストレージサブシステム及びストレージサブシステム内の記憶領域へのアクセスを選択的に制限することにより、不正アクセスを防止できるストレージサブシステムに関する。
【０００２】
【従来の技術】ANSI X3T11で標準化されたファイバチャネルプロトコルでは、多数の装置が接続可能であり、かつSCSI、ESCON、TCP/IP等多種のプロトコルを同時に運用可能な利点があるが、それに伴いセキュリテイの確保が困難となる性質も併せ持っている。
【０００３】ストレージサブシステムに対する不正アクセスを防止する方法としては、例えば特開平10-333839号公報では、ファイバチャネルプロトコルを用いた方法が開示されている。
【０００４】この方法は、装置のインタフェース（ポートと呼ぶ）を、静的に一意に識別できるN_Port_Nameについて、上位装置を起動する前に予めストレージサブシステム中に記憶させ、かつこのN_Port_Nameと、ストレージサブシステム中の特定ポート、或いはN_Port_Nameとストレージサブシステム内部の任意の記憶領域とを関連付けるテーブルを保持し、上位装置起動後は、この上位装置がストレージサブシステムにアクセスする際に発行するフレームという情報単位の内部を、ストレージサブシステムにおいてフレーム毎に逐一判定して、フレーム内に格納されたN_Port_Nameがテーブル内に存在する場合にアクセスを許可し、存在しない場合はLS_RJTという接続拒否のフレームを上位に対して送出することによ

って、前記テーブル内に存在しないN_Port_Nameをもつ上位装置からのアクセスを拒否するというものである。

【0005】

【発明が解決しようとする課題】しかし上記方法では、第一に接続可否の判定をフレーム毎に行う必要があるために通信性能が大幅に制限されること、第二にアクセス可否の対象がポートではなくストレージサブシステム内の部分領域である場合、上位装置から送出されるフレームすべてにN_Port_Nameを格納することが上位装置に要求されるため、上位装置側に標準ファイバチャネルプロトコル範囲外の仕様の実装を強いることから、実際の製品に適用することは困難である。

【0006】本発明はANSI X3T11で標準化されたファイバチャネルプロトコルを上位装置とのインタフェースとしてもつストレージサブシステムにおいて、上位装置からストレージサブシステム内の記憶領域へのアクセスを選択的に制限することにより、不正アクセスを防止することを目的とする。

【0007】またこの際、アクセスの可否を判定する際生じるオーバヘッドが最小限となる方法を提供し、かつ判定の条件を標準ファイバチャネルプロトコルの範囲のみで行える方法を提供することを目的とする。

【0008】

【課題を解決するための手段】上記課題を解決するために、上位装置又は上位装置のポートを静的に一意に識別する識別手段であるN_Port_Name或いはNode_Nameと、ストレージサブシステム内におけるアクセス可否判定の対象である各記憶領域とを対応づけたテーブルをストレージサブシステム内に保持し、さらにN_Port_Name或いはNode_Nameと、上位装置がファイバチャネルインタフェースを用いてストレージサブシステムと通信を行う際に、上位装置又は上位装置のポートを一意に識別する手段として、情報の送受信に先立つログインプロセスにより動的に割り当てられる情報であるS_IDとを関連付けたテーブルをストレージサブシステム内に保持し、上位装置からストレージサブシステム内の記憶領域に対する情報取得要求が、Inquiryコマンドを用いて行われた契機で、要求フレームに含まれるS_IDを用いて、上記テーブルを検索及び比較することによって記憶領域に対するアクセス可否を判定する。

【0009】

【発明の実施の形態】以下、本発明の実施の形態について、図を用いて詳細に説明する。まず、本発明で使用するファイバチャネルの特徴について説明する。

【0010】ファイバチャネルは、独自のコマンドセットを持たないシリアルの転送方式をもつプロトコルであり、情報を非同期に送るために伝送媒体の帯域幅を有効に利用できる特色を持っている。そして独自のコマンドセットを持たないかわりに、物理転送方式を、従来のSCSI、ESCONといったコマンドセットの運搬路として使用することにより、従来のソフトウェア資産を継承しながら、より高速かつ多彩なデータ転送を可能としている。

【0011】ファイバチャネルはチャネルとネットワークの特長を併せ持つインタフェースである。すなわち、ファイバチャネルでは一旦転送元と転送先が確定すれば、遅延が少ない高速な転送が行える。これはチャネルの特長である。また、通信を希望する機器は、任意の契機でファイバチャネルの通信系に参加し、通信の目的となる相手の機器と相互に情報を交換することにより、互いを認識して通信を開始することができる。これはネットワークの特徴である。ここで述べた相手の機器との情報交換の手続きを、とくにログインと呼ぶ。

【0012】ファイバチャネルのインタフェースを持つ機器をノードと呼び、実際のインタフェースにあたる部分をポートと呼ぶ。ノードは1つ以上のポートを持つことが可能である。ファイバチャネルの系全体に同時に参加できるポートの数は、最大で24ビットのアドレスの数すなわち約1677万個である。この接続を媒介するハードウェアをファブリックと呼ぶ。送信元及び送信先のポートは、ファブリックを意識せずに互いのポートに関する情報のみを考慮して動作すればよいので、ファブリックを論理的な媒体として議論する場合も多い。

【0013】各ノード及びポートには、標準化団体から一定のルールによって割り当てられる世界中でユニークな識別子が記憶されている。これはTCP/IPのMACアドレスに相当するものであり、ハードウェア的に固定なアドレスである。このアドレスにはN_Port_Name、Node_Nameの2種類があり、それぞれ8バイトの領域を持つ。N_Port_Nameはポート毎に固有の値、Node_Nameはノード毎に固有の値となる。

【0014】ファイバチャネルでは、通信はOrdered Setと呼ばれる信号レベルの情報と、フレームと呼ばれる固定のフォーマットを持った情報とで行われる。

【0015】図1はこのフレームの構造を示している。フレーム101は、フレームの始まりを示すSOF（Start of Frame）102と呼ばれる4バイトの識別子、リンク動作の制御やフレームの特徴づけを行う24バイトのフレームヘッダ103、実際に転送される目的となるデータ部分であるデータフィールド104、4バイトの巡回冗長コード（CRC）105、フレームの終わりを示すEOF（End of Frame）106と呼ばれる4バイトの識別子からなる。データフィールド104は0～2112バイトの間で可変である。

【0016】次に、図2を用いてフレームヘッダの内容について説明する。図2はフレームヘッダの構造について示している。ここではフレームヘッダ202の詳細構造203における、1ワードの23-0ビット領域にあたるS_ID204のみ説明する。S_ID（Source ID）204は当該フレームを送信するポートを識別するための3バイトのアドレス識別子であり、送受信されるすべてのフレームで有効な値を持つ。そして上位装置を動的に一意に識別できる情報

であり、PLOGI時（後述）に上位装置より報告される値である。このS_IDは動的に変動する値であり、FC_PHではファブリックによって初期化手続き時に割り当てられることになっている。割り当てられる値は、それぞれのポートが持つN_Port_Name、Node_Nameに依存する。

【００１７】次に、送信元の機器と送信先の機器が互いに情報を交換する、ログイン手続きについて述べる。図3に、上位装置からストレージサブシステムへの通信要求であるPLOGIフレームの構造について示す。フレームヘッダ302の詳細構造304において、ワード1の23-0ビットがS_ID306である。また、データフィールド303の詳細構造305において、先頭から21バイト目～29バイト目までの8バイトの領域がN_Port_Name307を格納する領域であり、先頭から30バイト目～38バイト目までの8バイトの領域がNode_Name308を格納する領域である。

【００１８】図4は、送信元（ログイン要求元）と送信先（ログイン要求先）との間に取り交わされる情報を示したものである。ファイバチャネルのログイン手続きには数種類があるが、ここではクラス３のログインで取り交わされる情報を示す。

【００１９】ログイン要求元は、PLOGIフレーム403をログイン要求先へ送信する。このフレームには、ログイン要求元のN_Port_Name、Node_Name、S_ID及びその他の情報が含まれている。要求先の装置では、このフレームに含まれている情報を取り出し、ログインを受諾する場合はACC404と呼ばれるフレームをログイン要求元に対して送信する。

【００２０】ログインを拒絶する場合は図5に示すように、PLOGIフレーム503に対して、ログイン受信先はLS_RJT504と呼ばれるフレームをログイン要求元に対して送信する。

【００２１】ログイン要求元は、自らが送信したPLOGIフレームに対するACCフレームの応答を受信すると、ログインが成功したことを知り、データ転送などのI/Oプロセスを開始できる状態となる。LS_RJTを受信した場合はログインが成立しなかったため、ログイン要求先へのI/Oプロセスは不可となる。ここではクラス３のログインについて述べたが、他のログインにおいても、ログイン要求元からログイン要求先へ渡すことのできる情報の中に、N_Port_Name、Node_Name及びS_IDが含まれることは同様である。

【００２２】次に、Inquiryコマンドについて説明する。Inquiryコマンドとは、I/Oプロセスを開始しようとする場合に先立ち、プロセスの対象となる論理デバイスに対して、その実装状態を問い合わせるコマンドである。例えば、上位装置からストレージサブシステムに含まれる記憶領域へのアクセス要求に先立つ情報問い合わせ要求のことである。本コマンドはSCSIでは必ずサポートされている標準コマンドである。

【００２３】図6は、SCSI規格で定義されたInquiryコマンドを、ファイバチャネル規格のフレームで送信する場合のフレーム601のフォーマットである。フレームヘッダ602の詳細構造604において、本フレームに先立つPLOGIで割り当てられたS_ID605が含まれている。データフィールド603にはFCP_LUN607、FCP_CNTL608、FCP_CDB609、FCP_DL610と呼ばれる領域がある。ここではFCP_LUN607、及びFCP_CDB609について述べる。

【００２４】FCP_LUN607の中には、フレーム送信元が状態を問い合わせようとする、フレーム送信先のポートに関連付けられた論理ボリュームの識別子が格納されている。この識別子をLUNという。FCP_CDB609の中には、SCSIコマンドセットを使用する場合にはSCSIのコマンド記述ブロック（CDB）と呼ばれる命令情報が格納される。このFCP_CDB609の中に、SCSIのInquiryコマンド情報が格納されて、前述のFCP_LUN607と共に、フレーム要求先へ情報が転送される。

【００２５】次に、Inquiryコマンドを受信したフレーム要求先が、問い合わせへの応答としてフレーム送信元へ返信する情報について述べる。この情報をInquiryデータと言う。図7にInquiryデータの抜粋を示す。ここでは、Inquiryデータ701のうちでクオイファイア702と、デバイス・タイプ・コード703の２つについて述べる。クオリファイア（Peripheral Qualifier）702は、指定された論理ユニットの現在の状態を設定する3ビットの情報である。

【００２６】図8はビットパターンによって示される論理ユニットの状態を列挙したものである。コード000（2進）802は、論理ユニットとして接続されている装置がデバイス・タイプ・コード703の領域に示される種類の入出力機器であることを示している。本コードが設定されていても、その論理ユニットが使用可能、すなわちレディ状態であることを必ずしも示しているわけではないが、その論理ユニットを使用できる可能性があるのは本コードが設定されている場合に限る。

【００２７】コード001（2進）803は、論理ユニットとして接続されている装置がデバイス・タイプ・コード703の領域に示される種類の入出力機器であることを示しており、かつそのロジカルユニットには実際の入出力機器が接続されていないことを示している。これは例えばCD-ROMドライブが実装されているが、CD-ROMがドライブ内に挿入されていないような場合を示すことになる。コード011（2進）804は、指定された論理ユニットがサポートされていないことを示す。従って指定された論理ユニットに装置が割り当てられることはない。本コードが設定されるときは、デバイス・タイプ・コード領域703にはかならず1F（16進）が設定されることが条件になっている。

【００２８】デバイス・タイプ・コード（Peripheral Device Type）703は、指定された論理ユニットに実際に割り当てられている入出力機器の種別を示す5ビットの

情報である。

【００２９】図9に各デバイスタイプ902に対応するに16進のコード901を示す。図9に示されている情報のうち、未定義又は未接続のデバイス903を表す1F（16進）904が設定されると、Inquiryコマンド送信元が問い合わせたデバイスは未定義或いは未接続ということになり、当該論理ユニットは当該送信元からは使用できないことになる。

【００３０】図10に、このInquiryコマンドを用いた論理ユニット問い合わせの手順を示す。論理ユニットにアクセスしようとする上位装置1001は、アクセスしようとする論理ユニットをもつストレージサブシステム1002に対し、Inquiryコマンドを含むフレーム1003を送信する。このフレームには、PLOGIで割り当てられた、上位装置のS_IDと、問い合わせを行う論理ユニットの識別子であるLUNが含まれている。なおここで、LUNについては、FCP_LUN領域の他に、FCP_CDB内のInquiryコマンド情報そのものの中にも設定することができる。どちらの値を使用しても得られる効果は同じであるが、本実施例ではLUNの値はFCP_LUNに格納された値を使用するものとする。

【００３１】Inquiryコマンドを含むフレームを受信したストレージサブシステム1002は、問い合わせに対する返答に必要なInquiryデータを準備し、作成したInquiryデータを含むフレーム1004を上位装置に対して送信する。このときInquiryデータを格納するフレームを、FCP_DATAと呼ぶ。このとき、ストレージサブシステムが、問い合わせのあったロジカルユニット（論理ユニット）について、クオリファイア000（2進）、デバイスタイプ00～09（16進）のいずれかを設定した場合、このInquiryデータを受信した上位装置は、ロジカルユニットに対するI/Oを試みることが可能となる。

【００３２】また、図11に示すように、ストレージサブシステム1102が、クオリファイア001（2進）又は011（2進）、デバイスタイプ1F（16進）を設定した場合、このInquiryデータ1104を受信した上位装置は、ロジカルユニットに対するI/Oが不可能であることを検出する。これらのことから、Inquiryデータに格納するクオリファイア、及びデバイス・タイプ・コードを管理することによって、上位装置からのロジカルユニットへのアクセスの許可及び不許可を制御することが可能となる。

【００３３】本発明では、上位装置からのアクセスを許可、或いは拒否する対象として、ストレージサブシステム内の一定領域を選択することを可能としている。この領域は上位装置から明示的にアドレス指定が可能な領域であり、LU（Logical Unit）と呼ばれる。LUの識別子をLUN（Logical Unit Number）と呼ぶ。SCSI-2ではLUNの個数は1ターゲットあたり8である。

【００３４】次に、本発明による処理の流れについて説明する。

【００３５】図12は、本発明の実施例となる装置の構成図である。本装置をストレージサブシステム1201と呼ぶ。ストレージサブシステム1201は、複数のファイバチャネルインタフェースを持つポート1202によって上位装置（ホストと呼ぶ）1203と接続されている。接続形態はファイバチャネル規約によりさまざまであるが、本発明では接続形態を問わないため一括してファイバチャネル1204として表記してある。

【００３６】上位装置1203もまたファイバチャネルインタフェースを持つポート1205を1つ以上備えており、それぞれのポート1205がストレージサブシステム1201上のポート1202とファイバチャネルプロトコルにより通信可能である。

【００３７】ストレージサブシステム1201は中央演算装置1206を持ち、各種処理を行う。またストレージサブシステム1201は内部に不揮発メモリ1207を備えている。この不揮発メモリ1207は各種テーブルやN_Port_Name或いはNode_Nameを保持する保持手段としての役割を果たす。デバイスドライブ制御部1208はバス1209を介して情報を記憶しているドライブデバイスと接続されている。本図ではドライブデバイスを論理単位としてとらえ、論理ユニット（LU）1210として表示している。

【００３８】また、ストレージサブシステム1201は通信制御部1211を持ち、通信回線1212を介して保守用装置1213の通信制御部1214と情報の送受信を行うことができる。保守用装置1213とは例えばパソコンのようなものであり、中央演算装置1215と入力手段1216及び表示手段1217を持つ。ユーザはこの保守用装置1213を用いて、ストレージサブシステム1201の保守を行う他、N_Port_Name或いはNode_NameとLU1210の特定の記憶領域とを関連付け上位装置1203に対するアクセス可否を定義した情報（アクセス可否テーブル）を設定する。このように保守用装置1213は設定手段の役割も果たす。不揮発メモリ1207はこのように定義したアクセス可否テーブルをN_Port_Name或いはNode_Nameと共に保持する。

【００３９】更に不揮発メモリ1207は、中央演算装置1215で作成する関連テーブル（上位装置1203からストレージサブシステム1201への通信要求であるPLOGIを受け付けた際に、N_Port_Name或いはNode_Nameと上位装置1203とを動的に一意に識別できる情報であり、PLOGI時に上位装置1203より報告される値であるS_IDとを関連付け、このS_IDを不揮発メモリ1207内に保持してあるN_Port_Name或いはNode_Nameと関連付けたテーブル）を保持する。

【００４０】図13は、本発明によるLUNセキュリティの実現方法の概要を説明したものである。まず手順1301では、ユーザは予めホストが持つN_Port_Nameを用いて、ストレージサブシステムの各ポート毎に関連付けられたLUNと、そこにアクセスしうるホストのN_Port_Nameを結び付けたアクセス可否テーブルを保守用装置（図12参

照）などを用いて作成し、ストレージサブシステム内の記憶領域（図12に示す不揮発メモリ等）に保持する。ここで得られるN_Port_Nameは既知であるとする。

【００４１】次に、手順1302において、ホストがストレージサブシステムに対してログインを行う。ストレージサブシステムは、このログインのPLOGIフレームからホストのN_Port_Name及びS_IDを取り出し、N_Port_NameとS_IDとを関連付けた関連テーブルを作成する。作成された関連テーブルは、先のアクセス可否テーブルと同様にストレージサブシステム内の記憶領域に保持される。

【００４２】次に、手順1303に移り、ホストはストレージサブシステム内の論理ユニットの状態を検査するためにInquiryコマンドを送信する。このInquiryコマンドを受信したストレージサブシステムは、Inquiryコマンドを格納しているフレームのヘッダからS_IDを取り出し、また同フレームからInquiryコマンドの対象となるLUNを取り出す。そして関連テーブルを使用して、S_IDからN_Port_Nameを割り出し、さらにアクセス可否テーブルからそのLUNがN_Port_Nameに対してアクセス許可されているか、もしくは不許可であるかの情報を取得する。

【００４３】許可か不許可かの情報を用いて手順1304で中央演算装置はアクセス可否の判定をおこなう。結果が許可であった場合は、手順1305においてInquiryデータにＬＵが実装であることを設定し、不許可であった場合は、手順１３０７においてInquiryデータにLUが未実装であることを設定し、ホストに対して送信する。Inquiryデータを受信したホストはデータを解析し、対象LUが実装である、すなわち対象LUへのアクセスが許可されていることをデータから得ると、手順1306に示すように、それ以降当該LUに対してのI/O要求を行うことが出来るようになる。

【００４４】対象LUが未実装であることを検出すると、以降当該LUへのI/O要求へのI/O要求を行うことはできない。以上の手順により、ストレージサブシステム内のLUに対するセキュリティの管理が実現できたことになる。

【００４５】尚、N_Port_Namの代わりにNode_Nameを用いた場合も同様である。また、アクセス可否の判断は中央演算装置ではなく、専用の処理装置を設けて判断手段としてもよい。

【００４６】次に、各手順について詳細に説明する。

【００４７】まず、最初の手順であるN_Port_NameとLUNとの対応づけを行うテーブル作成手順について説明する。

【００４８】本発明におけるLUNに対するセキュリティ情報は、ストレージサブシステムに存在するポートを単位として管理されるものとする。つまり、論理ユニットLUは各ポートに対して定義され、ホストはこれらのポートを通してLUへアクセスする。したがって、セキュリティ情報もポート単位で管理されることになる。この場合必要な情報は、ホストを一意に特定できる情報、各LUの識別子であるLUN、及びLUNに対するアクセスの可否を示す状態ビットである。

【００４９】ホストを一意に特定できる情報とは、この時点ではN_Port_Nameとなる。N_Port_Nameは、ホストに存在するポート毎にユニークな値であるので、本発明によればホストのポート毎に、ストレージサブシステムのポートにおけるLUに対するセキュリティを設定できることになる。N_Port_Nameの替わりに、Node_Nameを使用したテーブルを作成すれば、ポスト毎にセキュリティを設定することになる。LUに対するアクセス権限を与える対象がホストのポート毎であるか、ホスト毎であるかの相違であるので、本実施例ではN_Port_Nameについて説明する。すなわち本実施例ではホストのポート毎にセキュリティを設定する方法を述べるが、N_Port_Nameの記述をNode_Nameに読み替えることによって、容易にホスト単位のセキュリティ設定方式を得ることができる。また、本実施例では、ホスト上にあるポートのことを、簡略化のためにホストと呼ぶことにする。つまり、ホストという語はホストそのものと、ホスト上に存在するポートの双方、或いはいずれかを意味することになる。

【００５０】図14に、本実施例で作成するアクセス可否テーブルを示す。本テーブルはストレージサブシステム上にあるポート毎に作成される。作成はストレージサブシステムと通信可能な保守用の装置から、入力手段とその入力結果を確認するための表示手段を用いて指示することにより行う。通信回線の種類により、LANを用いればストレージサブシステムに近い場所からの設定、電話回線を用いれば保守センタ等遠隔地からの設定が可能である。また内部バスを用いて保守用装置とストレージサブシステムを一体化させることも可能である。

【００５１】LUN1402はポートに関連付けられたLUを示し、N_Port_Name1403の数はそのポート配下に存在するLUへアクセスする可能性のあるホストの数だけ存在する。LU及びホストの数は有限な数となる。テーブルの各要素において、本実施例では値"1"がアクセス許可を、値"0"がアクセス拒否を意味することにする。図14では当該ポートにおいて、LUN 0へアクセス許可があるホストは、N_Port_Name "0123456789ABCDEF" 1409 をもつホストのみであり、LUN 1 1405へアクセス許可があるホストは、N_Port_Name "01234567 89ABCDEE" 1410及び "01234567 89ABCDED" 1411をもつホストである。またLUN n-1 1407へのアクセスが許可されているホストは存在しない。

【００５２】図15に示すように、本テーブルは、セキュリティの設定が必要なポートすべてについて作成し、ストレージサブシステム内の記憶領域に保持する。このとき記憶領域に不揮発記憶領域を使用すれば、ストレージサブシステムの電源が切断された場合でも情報を保持することができる。また、初期値を0又は1としてテーブルを作成しておくことにより、テーブル作成を簡略化する

ことができる。

【００５３】次に、ホストからのログインの手順について詳細に説明する。本手順ではPLOGIに伴う情報から、ホストのN_Port_NameとホストのS_IDを結び付ける処理を行う。

【００５４】まず、図16の手順1602に示すように、ホストからのログイン手続きとして、PLOGIフレームが送信される。手順1603においてストレージサブシステムでは、PLOGIフレームのヘッダから、ホストのS_IDを取得する。また同時に、手順1604において、PLOGIフレームのデータ領域から、ホストのN_Port_Nameを取得する。手順1605において、この2つの値を結び付け、図17に示すような関連テーブルを作成する。PLOGIはホストのポートと、ストレージサブシステム上のポートとの間で交わされるログインであるので、本テーブルもストレージサブシステムのポート毎に作成されることになる。

【００５５】手順1606でテーブルを更新することによって、本テーブルを用いて、S_ID1701が与えられれば該当するN_Port_Name1702を得ることが可能となる。本テーブルも、ストレージサブシステム内の記憶領域に保持されることは図14で示したテーブルと同様である。ホストに対しては、手順1607でPLOGIに対する応答としてACCと呼ばれるフレームを送信し、ホストにログインが受理されたことを通知する。ACCフレームを受信したホストは、以降当該ポートに対してのInquiry等を発行することができるようになる。

【００５６】次に、ホストからのInquiryコマンドの送信と、それに伴うセキュリティの応答について図18を用いて詳細に説明する。Inquiryコマンドは、FCP_CMNDと呼ばれる情報単位を含むフレームとしてホストからストレージサブシステムへ送信される。手順1802でホストからのデータフィールド内のFCP_CMNDフレームを受信したストレージサブシステムは、手順1803でFCP_CMNDフレームの内容を解析する。FCP_CMNDがInquiryコマンドでない場合は、それぞれに応じた処理1805に分岐する。FCP_CMNDがInquiryコマンドであった場合は、手順1806に遷移し、当該フレームからS_IDを切り出す。また、同時に手順1807にてFCP_LUNからInquiryが対象としているLUNを取り出す。

【００５７】次に、手順1808に移り、フレームから切り出したS_IDから、図17で示したテーブルを用いてN_Port_Nameを求める。さらに、求めたN_Port_Nameについて、図14で示したテーブルより、Inquiryコマンドが対象としているLUNについて、セキュリティを示したビットの状態を取得する。この時ホストから得られたS_IDが、FFFF01であり、Inquiryの要求するLUNが0であったとする。まず手順1808にて、図17に示すテーブルよりS_IDFFFF01 1703に対応するN_Port_Name "01234567 89ABCDEF" 1706 を取得した後、手順1809に移り図14に示したテーブルよりN_Port_Name"01234567 89ABCDEF" 1409 に対するLUN 0 1404のセキュリティ "1" を得る。

【００５８】セキュリティ "1" は本実施例ではアクセス許可を意味するので、手順1811に分岐し、ホストへ報告するInquiryデータとして、クオリファイアに000（2進）、デバイスタイプに当該デバイスに対応するコードをセットする。例えばストレージサブシステムがハードディスクアレイサブシステムである場合は、デバイスタイプは00（16進）となる。ついでInquiryデータを格納したフレームを作成し、手順1813でホストに対して送信をおこなう。さらに手順1814にて、返信が終了したことを示すFCP_RSPと呼ばれるフレームをホストに対して送信する。

【００５９】この一連の返信データを受け取ったホストは、Inquiryの結果として当該LUN=0のLUに対してアクセスができることを検知したことになるため、以降は次回のInquiryコマンドを受け付けるまで、当該LUに対してセキュリティのチェックを行う必要なくアクセスを行うことが可能となる。

【００６０】次にアクセスを拒否する場合を説明する。Inquiryコマンドの送信によりホストから得られたS_IDがFFFF01であり、Inquiryの要求するLUNが1であったとする。手順1808において、図17に示す関連テーブルよりS_IDFFFF011703に対応するN_Port_Name "01234567 89ABCDEF" 1706を取得した後、図14に示すアクセス可否テーブルよりN_Port_Name "01234567 89ABCDEF" 1409に対するLUN 1 1405のセキュリティ "0" を得る。

【００６１】セキュリティ "0" は本実施例ではアクセス拒否を意味するので、手順1812へ分岐し、ホストへ報告するInquiryデータとして、クオファイアに001（2進）又は011（2進）、デバイス・タイプ・コードに1F（16進）をセットしたInquiryデータを作成する。このInquiryデータを受信し、ついでFCP_RSPを受信したホストは、Inquiryの結果として当該LUN=1のLUが未実装であるという情報を得る。したがって、以降ホストは当該LUが実装されていないと判断するのでアクセス要求をすることはなくなる。

【００６２】以上のようにして、N_Port_Name、S_ID、LUNを用いたテーブルを保持することで、ストレージサブシステム側のポート毎に、ホストの各ポートに対しての各LUNへのアクセスについてのセキュリティを、ログイン及びInquiryの際に判断することで、効率よく行うことができる。

【００６３】

【発明の効果】本発明によって、上位装置から特定LUNに対するアクセスを、予め設定してあるN_Port_Name或いはNode_NameとLUNとのアクセス可否テーブル、PLOGIの際に判明するN_Port_Name或いはNode_NameとS_IDとの関係を用いて作成した関連テーブルの双方のテーブルを用いることによって、上位装置或いは上位装置のポートからのLUへの状態問い合わせがあった時点でアクセス可

否を決定し返答することができるため、ストレージサブシステムへのアクセス制限を、LUN単位で、しかも初回のみの判定プロセスで行うことができ、ファイバチャネル及びSCSIの規格上最も分解能の高いセキュリティを、高いパフォーマンスで確保することができる。

【図面の簡単な説明】

【図１】ファイバチャネルプロトコルにおけるフレームの構造図である。

【図２】フレームヘッダの構造図である。

【図３】PLOGIフレームの構造図である。

【図４】PLOGIが受諾されるシーケンス図である。

【図５】PLOGIが拒否されるシーケンス図である。

【図６】SCSIのInquiryコマンドを含むフレームの構造図である。

【図７】Inquiryデータの構造図である。

【図８】Inquiryデータ中クオリファイアの内容定義図である。

【図９】Inquiryデータ中デバイス・タイプ・コードの内容定義図である。

【図１０】InquiryデータにLU通常状態が設定される場合のシーケンス図である。

【図１１】InquiryデータにLU未定義状態が設定される場合のシーケンス図である。

【図１２】ストレージサブシステムの構成図である。

【図１３】全体シーケンスのフローチャートである。

【図１４】N_Port_Nameに対するLUアクセス可否の定義テーブルである。

【図１５】LUアクセス可否定義テーブルの設定フローチャートである。

【図１６】PLOGI処理のフローチャートである。

【図１７】ホストN_Port_NameとS_IDを関連付けるテーブルである。

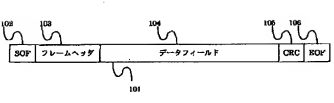
【図１８】Inquiryコマンド処理のフローチャートである。

【符号の説明】

101…フレーム、102…SOF（Start of Frame）、103…フレームヘッダ、104…データフィールド、105…CRC、106…EOF（End of Frame）、201…フレーム、202…フレームヘッダ、203…フレームヘッダ詳細、204…S_ID、301…フレーム、302…フレームヘッダ、303…データフィールド、304…フレームヘッダ詳細、305…データフィールド詳細、306…S_ID、307…N_Port_Name、308…Node_Name、401…ログイン要求元の動作、402…ログイン受信先の動作、403…PLOGIフレームの内容、404…ACCフレーム、501…ログイン要求元の動作、502…ログイン受信先の動作、503…PLOGIフレームの内容、504…LS_RJTフレーム、601…フレーム、602…フレームヘッダ、603…データフィールド、604…フレームヘッダ詳細、605…S_ID、606…データフィールド詳細（FCP_CMND）、607…FCP_LUN、608…FCP_CNTL、609…FCP_CDB（Inquiry）、610…FCP_DL、701…Inquiryデータ抜粋、702…クオリファイア、703…デバイス・タイプ・コード、801…クオリファイアの定義、802…000（2進）、803…001（2進）、804…011（2進）、901…デバイス・タイプ・コード（16進）、902…デバイス・タイプ、903…1F（16進）、904未定義又は未接続のデバイス、1001…上位装置（ホスト）のInquiry処理シーケンス、1002…ストレージサブシステムのInquiry処理シーケンス、1003…Inquiryを含むフレーム(FCP_CMND)に格納される情報、1004…デバイス通常状態を通知するInquiryデータ、1101…上位装置（ホスト）のInquiry処理シーケンス、1102…ストレージサブシステムのInquiry処理シーケンス、1103…Inquiryを含むフレーム(FCP_CMND)に格納される情報、1104…デバイス未定義状態を通知するInquiryデータ、1201…ストレージサブシステム、1202…ストレージサブシステムのファイバチャネルポート、1203…上位装置（ホスト）、1204…ホストとストレージサブシステムを接続するファイバチャネルプロトコル、1205…ホストのファイバチャネルポート、1206…中央演算装置、1207…不揮発メモリ、1208…デバイスドライブ制御部、1209…バス、1210…LU（論理ユニット）、1211…通信制御部、1212…通信回線、1213…保守用装置、1214…通信制御部、1215…中央演算装置、1216…入力手段、1217…表示手段、1301…全体手順1、1302…全体手順2、1303…全体手順3、1304…全体手順4、1305…全体手順5、1306…全体手順6、1307…全体手順7、1401…N_Port_Nameに対するLUアクセス可否定義テーブル、1402…LUN、1403…N_Port_Name、1404…LUN 0のLUに対する定義、1405…LUN1のLUに対する定義、1406…LUN 2のLUに対する定義、1407…LUN n-1のLUに対する定義、1408…LUN nのLUに対する定義、1409，1410，1411…N_Port_Name、1601…PLOGI処理フローチャート開始、1602…PLOGI処理手順1、1603…PLOGI処理手順2、1604…PLOGI処理手順3、1605…PLOGI処理手順4、1606…PLOGI処理手順5、1607…PLOGI処理手順6、1701…S_ID、1702…N_Port_Name、1703，1704，1705…S_ID、1706，1707，1708…N_Port_Name、1801…Inquiry処理フローチャート開始、1802…Inquiry処理手順1、1803…Inquiry処理手順2、1804…Inquiry処理手順3、1805…Inquiry処理手順4、1806…Inquiry処理手順5、1807…Inquiry処理手順6、1808…Inquiry処理手順7、1809…Inquiry処理手順8、1810…Inquiry処理手順9、1811…Inquiry処理手順10、1812…Inquiry処理手順11、1813…Inquiry処理手順12、1814…Inquiry処理手順13。

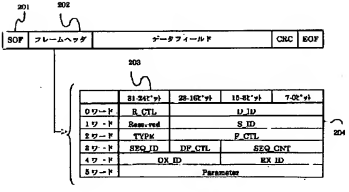
【図1】

図1



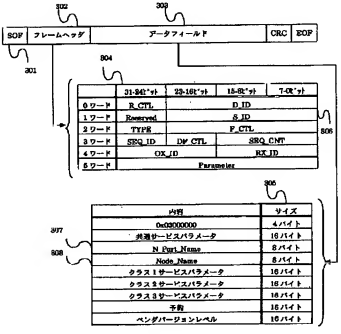
【図2】

図2



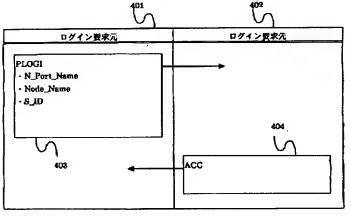
【図3】

図3



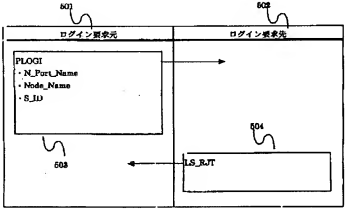
【図4】

図4



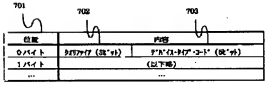
【図5】

図5



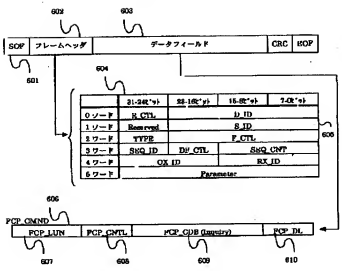
【図7】

図7



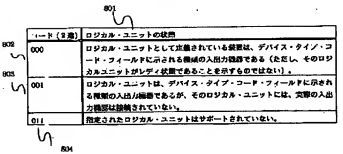
【図6】

図6



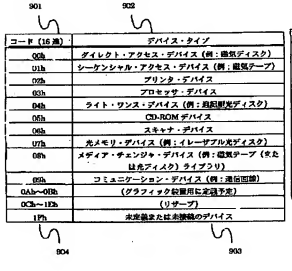
【図8】

図8



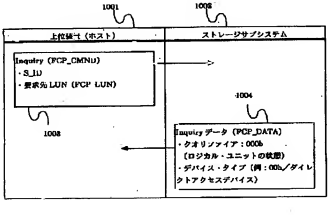
【図9】

図9



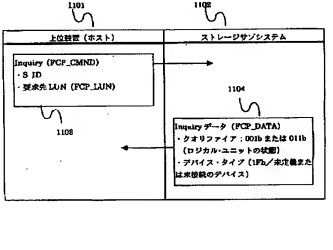
【図10】

図10



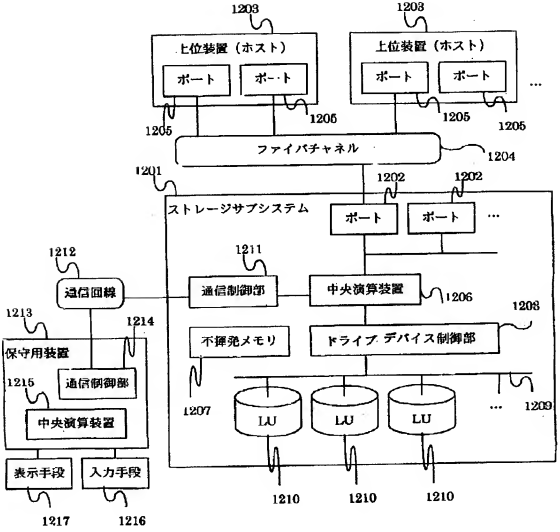
【図11】

図11



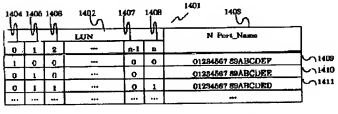
【図12】

図12



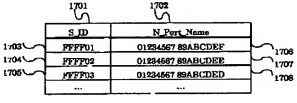
【図14】

図14



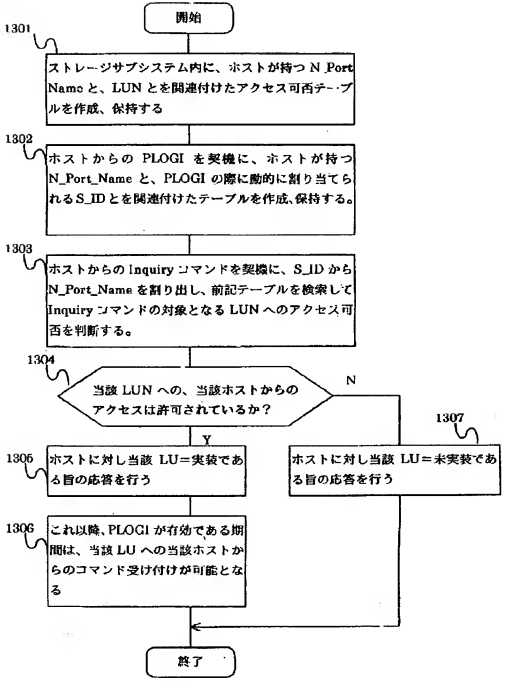
【図17】

図17



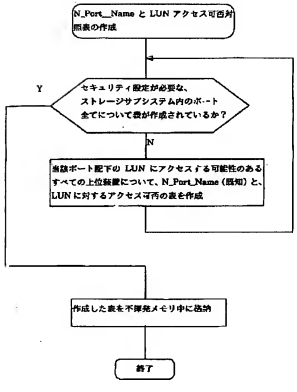
【図１３】

図 13


開始
1301
ストレージサブシステム内に、ホストが持つ N_Port Name と、LUN とを関連付けたアクセス可否テーブルを作成、保持する
1302
ホストからの PLOGI を契機に、ホストが持つ N_Port_Name と、PLOGI の際に動的に割り当てられる S_ID とを関連付けたテーブルを作成、保持する。
1303
ホストからの Inquiry コマンドを契機に、S_ID から N_Port_Name を割り出し、前記テーブルを検索して Inquiry コマンドの対象となる LUN へのアクセス可否を判断する。
1304
当該 LUN への、当該ホストからのアクセスは許可されているか？
N
Y
1307
ホストに対し当該 LU＝未実装である旨の応答を行う
1306
ホストに対し当該 LU＝実装である旨の応答を行う
1306
これ以降、PLOGI が有効である期間は、当該 LU への当該ホストからのコマンド受け付けが可能となる
終了

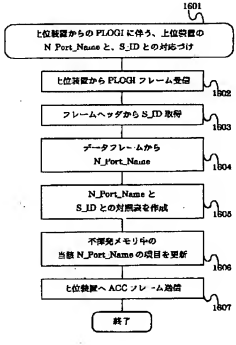
【図15】

図15



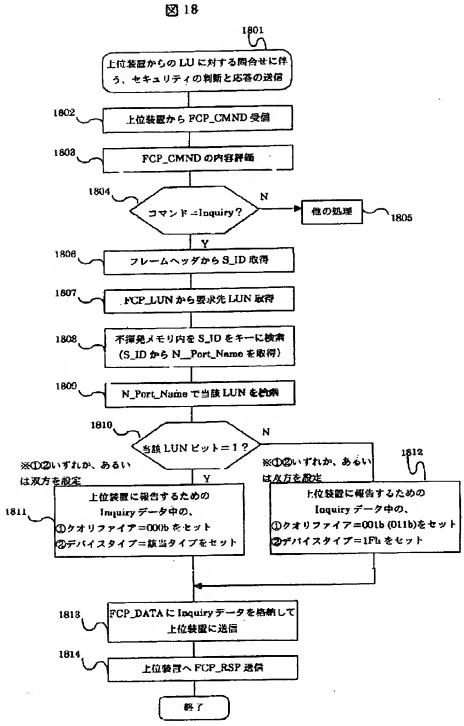
【図16】

図16



【図18】

図 18


1801
上位装置からのLUに対する問合せに伴う、セキュリティの判断と応答の送信
1802
上位装置からFCP_CMND受信
1803
FCP_CMNDの内容評価
1804
コマンド=Inquiry?
N
他の処理
1805
Y
1806
フレームヘッダからS_ID取得
1807
FCP_LUNから要求先LUN取得
1808
不揮発メモリ内をS_IDをキーに検索(S_IDからN_Port_Nameを取得)
1809
N_Port_Nameで当該LUNを検索
1810
当該LUNビット=1?
N
※①②いずれか、あるいは双方を設定
Y
1811
上位装置に報告するためのInquiryデータ中の、
①クオリファイア=000bをセット
②デバイスタイプ=該当タイプをセット
1812
※①②いずれか、あるいは双方を設定
上位装置に報告するためのInquiryデータ中の、
①クオリファイア=001b (011b)をセット
②デバイスタイプ=1Fhをセット
1813
FCP_DATAにInquiryデータを格納して上位装置に送信
1814
上位装置へFCP_RSP送信
終了